

INTERNT UDKAST

Sikkerhed i lægepraksis

Praktisk vejledning

Version 2.0

Sikkerhed i lægepraksis

Praktisk vejledning

Version 2.0

©UNI•C december 2011

Martin Bech og Tonny Bjørn

Indhold

1	Forord.....	1
1.1	Formål med vejledning i sikkerhed i lægepraksis.	1
2	It i lægepraksis	2
3	Eksterne opkoblinger i lægepraksis	3
3.1	Forbindelse til VANS-nettet for EDIFACT-meddelelser.....	3
3.2	Forbindelse til systemleverandør og sundhedsdatanettet....	3
3.3	Forbindelse til internettet	3
3.4	Forbindelse til hjemmearbejdsplads	3
3.5	Risikoanalyse	4
4	Trusler mod datasikkerheden indefra.....	6
4.1	Sikring mod tyveri og fysiske skader	6
4.1.1	Hardware	6
4.1.2	Datamedier og systembeskrivelser	6
4.1.3	Nødprocedurer ved fysiske skader	6
4.1.4	Backup.....	6
4.2	Sikring mod misbrug på det lokale net	7
4.2.1	Netværkskomponenter.....	7
4.2.1.1	Servere	7
4.2.1.2	Arbejdsstationer.....	7
4.3	Adgangskontrol	7
4.3.1	Administration af brugere.....	7
4.3.2	Sådan laver man et godt kodeord	8
4.3.3	Brug af pauseskærm	8
5	Trusler mod datasikkerheden udefra	9
5.1	Global netværksstruktur	9
5.2	Datasikkerhed på internettet.....	9
5.2.1	Router	9
5.2.2	Firewall.....	9
5.2.3	Personlige Firewalls	9
5.3	Trusler fra internettet	10
5.3.1	Virus	Fejl! Bogmærke er ikke defineret.
5.3.2	Port-scanning	10
5.3.2.1	Starten på et hackerangreb?.....	10
5.3.2.2	Sikring mod portscanning	10

5.3.2.3 Sårbarhed og opdatering	11
5.3.3 Sniffing	11
5.3.3.1 Hvordan sniffer man?	11
5.3.4 Kryptering	11
6 Driftssikkerhed.....	13
6.1 Beskrivelse af ansvar og opgaver.....	13
6.2 Virusberedskab	13
6.3 Dokumentation	13
7 Ordliste.....	14

1 Forord

1.1 Formål med vejledning i sikkerhed i lægepraksis.

Sikkerhed er et meget centralt punkt i forbindelse med it-anvendelser i lægepraksis. Sikkerhed er samtidig en kompliceret disciplin, som kræver, at alle involverede parter arbejder sammen om at etablere sikkerhedsmæssige rammer, så både læger og personale trygt kan udføre deres arbejde. Dette sker bedst, hvis lægepraksis er opmærksom på sikkerhed og følger de vejledninger, der findes på området.

Denne vejledning for sikkerhed i lægepraksis skal ses som en hjælp til lægepraksis i denne proces. Det er samtidig vigtigt at understrege, at der er tale om praktisk vejledning, der fokuserer på procedurer, der er vigtige for sikkerheden. Følges vejledningen vil lægepraksis været nået langt, men selv om vejledningen følges, vil det ikke være en garanti for, at der ikke kan ske sikkerhedsbrist.

Sikkerhedspolitikken bliver til stadighed påvirket af nye løsningsmuligheder og nye forsøg på kompromittering. Sikkerhedsområdet er under hastig udvikling, og vejledning for lægepraksis skal afspejle dette for ikke at give en falsk tryghed. Lægepraksis skal således sikre sig mod angreb udefra, fx sikre at klinikkens server ikke benyttes eller kontrolleres af personer, som ikke har autorisation til dette; sikre at e-mail håndteres som fortroligt, så den ikke læses eller forvanskes af uvedkommende; sikre sig mod virusangreb osv. Lægepraksis skal samtidig også feje for egen dør, så ingen med tilknytning til lægepraksis misbruger netadgang og it-systemer.

Denne vejledning skal opfattes som en samling anbefalinger, der er særligt aktuelle i forbindelse med opkobling til det fælles sundhedsdatanet, og er altså ikke ment som en erstatning for de love, regler og vejledninger, der kommer fra officielt hold - såsom Sundhedsstyrelsen, Datatilsynet m.fl. Vejledningen har heller ikke til formål at anbefale lægepraksis specifik produceret hardware og -software eller andet udstyr.

2 It i lægepraksis

I lægepraksis anvendes it i forbindelse med sygdomsbehandlingen. Læger har jf. Sundhedsstyrelsens cirkulære nr. 235 af 19. december 1996 pligt til at føre ordnede optegnelser (journalføring), og til denne journalføring anvendes it-systemer. Men it anvendes også i forbindelse med kommunikation ud af huset i forbindelse med recepter, indlæggelsesskrivelser til sygehuse m.m. og til rent administrative formål så som administration af tidsbestillinger og afregninger med sygesikringen.

It-anvendelserne i lægepraksis vil normalt være baseret på færdige systemer, der er udviklet af lægesystemleverandører, og lægesystemerne vil være udviklet til at køre decentralt dvs. på et par arbejdsstationer og en server, der i lægepraksis er forbundet i et lokalnetværk. Fra lokalnetværket skal der etableres eksterne forbindelser til andre parter inden for sundhedssektoren og til myndighederne. For lægepraksis er der behov for at kunne etablere en række forbindelser så som:

- til VANS-nettet for edifact meddelelser.
- til sundhedsdatanettet for Web-opslag til f.eks. laboratorieopslag og edi-mail (personhenførbare data).
- til internettet for Web-opslag og e-mail (ikke personhenførbare data).
- til praksislægens hjemmekontor.

I forbindelse med etablering af eksterne forbindelser er det meget vigtigt at tage de nødvendige sikkerhedsmæssige hensyn, således at det undgås, at udeforstående uretmæssigt får adgang til data i lægepraksis, eller andre steder via udstyret i lægepraksis.

Nogle af de forholdsregler, der beskrives i det følgende er mest relevante hvis servere og data befinder sig i klinikken. Hvis mange af disse ting befinder sig hos en lægesystemleverandør og man i klinikken kun har pc'er, der bruges som terminaler, varetages backup f.eks. af lægesystemleverandøren. Under alle omstændigheder vil mange af anbefalingerne i det følgende være relevante og for hvert punkt bør man overveje i hvad omfang det er aktuelt for ens egen situation.

3 Eksterne opkoblinger i lægepraksis

3.1 Forbindelse til VANS-nettet for EDIFACT-meddelelser

Tilslutning til VANS-nettet i forbindelse med afsendelse/modtagelse af EDI-FACT-meddelelser sker i mange tilfælde ved, at lægepraksis selv etablerer modem- eller ISDN-forbindelse til en af de to VANS-leverandører. Der findes også løsninger, hvor lægepraksis afsender/modtager meddelelser på krypteret VPN-forbindelse til lægesystemleverandøren som så formaterer meddelelserne til EDI-FACT og sørger for den videre transport.

3.2 Forbindelse til systemleverandør og sundhedsdatanettet

For lægepraksis vil tilslutning til sundhedsdatanettet i de fleste tilfælde ske via lægesystemleverandøren.

For at kunne blive tilsluttet sundhedsdatanettet har lægesystemleverandøren måttet indgå en samarbejdsaftale med MedCom. De generelle vilkår i aftalen er både gældende for lægesystemleverandøren og lægepraksis.

Tilslutning til sundhedsdatanettets knudepunkt skal ske med en hardware-baseret VPN-løsning dvs. ikke VPN-klient. VPN-forbindelsen skal være krypteret og der skal foretages adressekonvertering (NAT) før VPN til sundhedsdatanettets interne IP-adresser.

Forbindelsen mellem lægepraksis og lægesystemleverandøren bør tilsvarende blive etableret som en krypteret hardware-baseret VPN forbindelse.

3.3 Forbindelse til internettet

Fra lægepraksis vil det normalt være muligt at foretage Web-opslag og at sende/modtage e-mail, dvs. at der fra lægepraksis er adgang til det åbne internet. Adgang fra lægepraksis til det åbne internet skal være beskyttet af firewall, der skal være sat op, således at det til det generelle internet kun er muligt at foretage udgående Web-opslag og at anvende e-mail.

3.4 Forbindelse til hjemmearbejdsplads

Forbindelse mellem lægepraksis (klinik) og hjemmekontor bør ske efter følgende retningslinier:

- Der skal etableres en krypteret VPN-forbindelse mellem klinik og hjemmekontor. En hardware baseret løsning vil være at foretrække, men det er ikke et krav.
- I forbindelse med, at hjemmekontoret kontakter klinikkens netværk, skal det undersøges, om brugeren (brugeridentifikation/kodeord) har lov at blive tilsluttet klinikkens netværk.
- En bruger, der tilslutter sig klinikkens netværk, skal være oprettet på klinikens server.
- Der bør installeres sikkerhedspakke på hjemme-pc'en som imødekommer de gældende trusler. Dennes signaturfiler skal opdateres dagligt.
- Der skal tages stilling til punkterne i Datatilsynets vejledning om hjemmearbejdspladser (se www.datatilsynet.dk under "Forside / Erhverv / Personale-administration / Hjemmearbejdspladser").

3.5 Risikoanalyse

Er lægepraksis (klinikken) beskyttet, som det er beskrevet i det foregående, kan læseren få den fejlagtige opfattelse, at så kan der ikke være problemer med sikkerheden. Det er imidlertid ikke tilfældet, og vi skal her se på følgende muligheder for kompromittering af sikkerheden:

- Fra lægepraksis er der åbnet op for Web-opslag og e-mail. Når en arbejdsstation i klinikken foretager Web-opslag eller modtager e-mail vil der altid være mulighed for, at vira eller andre uønskede programstumper ad denne vej kan komme ind på maskinen.
- Fra hjemmekontoret tilsluttes pc, der evt. ikke er beskyttet mod seneste trusler på internettet.

Det er derfor vigtigt at overholde følgende hovedregler i forbindelse med klinikken:

- Adgang til internettet fra lokalnetværket skal være beskyttet mod indkommende trafik med hardware-baseret firewall.
- Installer antivirus program, der både beskytter server og pc'er og sørg for daglig opdatering af antivirusprogrammets signaturfiler. Arbejds-pc'ere kan med fordel beskyttes med en komplet sikkerhedspakke.
- En pc, der er tilsluttet sundhedsdatanettet, skal være beskyttet mod indkommende trafik fra internettet f.eks. ved tilslutning til lægepraksis' lokalnetværk med hardware baseret firewall.
- En pc, der tilsluttes det åbne internet for Web-opslag må ikke indeholde personhenførbare data.

- Har man trådløst net, skal dette være krypteret, således at kun autoriserede pc'er kan komme på nettet. Tilbyder man netopkobling som en service for kunder/brugere, skal denne være helt separat fra klinikkens øvrige net.

For lægens (og andre ansattes) hjemme-pc gælder:

- Da pc'en vil blive tilsluttet det åbne internet for e-mail og Web-opslag er det meget vigtigt at få installeret en sikkerhedspakke, der automatisk henter opdateringer.
- Der skal på pc'en anvendes styresystem, der kræver log-on (brugeridentifikation/password) fx Windows 7. Årsagen til dette er, at hvis andre medlemmer af husstanden bruger pc'en, kan deres adfærd på internettet endnu lettere være med til at kompromittere sikkerheden på pc'en og de programmer som benyttes til den arbejdsmæssige anvendelse af pc'en.
- Hjemme-pc må ikke på samme tid være tilsluttet det åbne internet og klinikken. Dette vil skabe en sikkerhedsrisiko. Anvendes en VPN-klient til klinikken, skal VPN-klienten lukke for andre forbindelser. En bedre løsning vil være at opsætte firewall til at beskytte mod indkommende trafik og til at etablere VPN forbindelse.
- Overføres personhenførbare data til hjemme-pc'en, skal data overføres og lagres krypteret, og der skal udarbejdes særlige regler for pc'en jf. Datatilsynets vejledning.
- Forbindelsen til klinikken skal lukkes ned, når der ikke mere er behov for adgang.
- Når pc'en ikke anvendes, bør den lukkes ned.

En mere generel gennemgang af trusler mod datasikkerhed findes i de følgende kapitler.

4 Trusler mod datasikkerheden indefra

Man kan skelne mellem de trusler, der opstår lokalt i lægepraksis, og de trusler, der kommer udefra.

Dette kapitel beskriver de interne forhold. Datasikkerheden på det lokale net kan kompromitteres på flere måder. Men overordnet kan man placere de fleste anslag mod sikkerheden i følgende kategorier:

- Tyveri – af hardware og software
- Skade – fysisk ødelæggelse af hardware og software, ændring i konfigurationen
- Misbrug – uautoriseret adgang til informationer, misbrug af kapacitet.

4.1 Sikring mod tyveri og fysiske skader

4.1.1 Hardware

Firewall, router, servere, hubs, switche og krydsfelter skal være placeret i aflåste rum eller skabe (gerne kamera overvåget), som er indrettet specielt til dette formål, således at sikkerhed i lægepraksis ikke kan kompromitteres.

Men for at kunne spore maskinerne i forbindelse med et eventuelt tyveri, kan det anbefales at nummerere dem, samt på anden måde mærke dem. En mærkning af udstyret med lægepraksis' navn kan ske ved enten at brænde eller ætse klinikkens navn ned i overfladen.

4.1.2 Datamedier og systembeskrivelser

Sikkerhedskopier og dokumentationer, der er nødvendige ved en eventuel genopbygning af lokalnetværket, bør opbevares i et aflåst og brandsikret skab evt. et pengeskab i et andet lokale end der, hvor serverne er placeret.

4.1.3 Nødprocedurer ved fysiske skader

For at mindske tabene ved en skade på klinikkens it-installationer, fx ved brand, vandskade, tyveri eller lignende, bør der være udarbejdet et sæt nødprocedurer, som sikrer at tabene minimeres.

4.1.4 Backup

Det er vigtigt at have en fast procedure for at tage backup af data. En sådan procedure skal som minimum skabe klarhed over

- hvilke data der skal laves backup af
- hvor ofte der skal laves backup
- en kontrol af at backup-kopien er brugbar (data kan gendannes)

4.2 Sikring mod misbrug på det lokale net

4.2.1 Netværkskomponenter

4.2.1.1 Servere

I de fleste lokalnet vil der være opstillet servere som bl.a. har den funktion at håndtere de enkelte brugeres rettigheder. Det kan være rettigheder til, hvilke programmer der må afvikles, og hvilke dele af centrale harddiske man har læse- og skriverettigheder til. Endvidere benytter mange serveren til at autentificere brugere og logge deres adfærd, så eventuelle forsøg på at kompromittere enten lokalnet eller eksterne net kan spores.

Kun autoriseret personale må have adgang til at ændre i serverens opsætning og dermed i brugerrettighederne.

4.2.1.2 Arbejdsstationer

Arbejdsstationer kan sikres ved, at det ikke er muligt at boote fra arbejdsstationens USB/diskette/CD/DVD drev, hvilket vil gøre det umuligt at indlæse andre konfigurationer.

Såfremt der ønskes en maksimal sikkerhed på arbejdsstationerne, kan arbejdsstationen etableres som en terminalløsning, hvor alle data og opsætninger ligger på serveren.

4.3 Adgangskontrol

For at sikre at den enkelte bruger kun får adgang til de ressourcer, der er relevante for at kunne udføre sin arbejdsfunktion, bør serveren konfigureres således, at ethvert login er forbundet med en adgangskontrol. I nogle lægepraksis findes der i dag kun to typer af brugere: Læger og adm. personale.

Dette bør ændres til, at *alle* brugere har et personligt brugernavn og password, så man kan spore forsøg på kompromittering tilbage til oprindelsen.

4.3.1 Administration af brugere

Kun systemadministrator bør have mulighed for at oprette og slette brugere.

Det er vigtigt, at systemadministrator sørger for at nedlægge brugerkonti, når en given bruger holder op, sådan at brugerdata basen kun indeholder det nødvendige antal konti.

Da oprettelsen af brugere sker fra en administratorkonto, bør systemadministrator have en anden Bruger-ID, som kan benyttes til det daglige arbejde.

Systemadministrationsarbejde bør kun foregå fra arbejdsstationer på det netsegment, som serveren står på, for at undgå at brugernavn og kodeord bliver "sniffet" på nettet.

Brugernavn og kodeord bør udleveres personligt til brugerne. I forbindelse med udleveringen skal brugeren gøres bekendt med regelsættet for anvendelsen af brugerkontoen.

4.3.2 Sådan laver man et godt kodeord

Det er vigtigt at vælge et godt kodeord til de it-systemer, man skal have adgang til. Men hvad er et godt kodeord, og hvordan laver man et? Lad os tage udgangspunkt i kodeordet: Politi

Umiddelbart er det et godt kodeord, da det er let at huske. Men det har flere mangler: Det består kun af bogstaver; det er et almindeligt ord, som kan findes i en ordbog, og det består kun af seks tegn. Et godt kodeord skal:

- være en blanding af tegn, tal og henholdsvis store og små bogstaver
- ikke være et kendt ord, eller et kendt ord bagfra
- evt. være sammensat af ord
- være minimum 8 tegn
- være let at huske

Hvis vi anvender disse regler kan man nå frem til følgende kodeord:

Po+li-10 og Spis5fisk

Disse kodeord er stadig er let at huske for brugeren, men meget svære at gætte.

Når man har lavet sit kodeord, gælder følgende:

Kodeordet skal

- læres udenad
- ikke være skrevet ned
- ikke være gemt på elektronisk form
- være hemmeligt og personligt

For at understrege vigtigheden af at lave et godt kodeord, kan man kigge på nogle af de programmer, der bruges til at gætte et kodeord.

På www.hackersclub.com finder man nogle af de mest brugte kodeord-cracker programmer. Et af de bedste er programmet Cracker Jack, der bruges til at knække kodeord på UNIX-maskiner. Der findes dog mange andre, der let og frit kan hentes fra internet. Cracker Jack vil på en stor computer kunne afprøve flere millioner kodeord i sekundet.

4.3.3 Brug af pauseskærm

Den oprindelige idé med en pauseskærm var at fjerne billedet fra skærmen, når computeren ikke blev brugt. Så undgik man, at billedet "brændte" sig fast i det fluorescerende lag i skærmens billedrør.

I dag er pauseskærmen blevet en beskyttelse mod andre brugeres adgang til computeren, når man er logget på med sit personlige kodeord.

Pauseskærmen bruges, når man holder en kortere pause uden at være logget af netværket eller andre systemer. I disse tilfælde skal pauseskærmen aktiveres og være beskyttet med kodeord, så ingen uvedkommende kan få adgang til systemet. Det letteste er at konfigurere pc'en til automatisk at aktivere pauseskærmen efter få minutters inaktivitet.

5 Trusler mod datasikkerheden udefra

5.1 Global netværksstruktur

Internettet er en global netværksstruktur. Det betyder, at lægepraksis med tilslutning til internettet ikke bare bliver tilsluttet sundhedsdatanettet, men at man potentielt også er udsat for trusler om brud på sikkerheden fra hele verden.

Stort set alle arbejdspladser er i dag koblet op til internettet og overalt i samfundet har man lært at håndtere denne risiko. Når vi alligevel bruger plads på at behandle emnet her, er det fordi vi betragter sundhedsdatanettet som et lukket net med et meget højere niveau af sikkerhed end internettet generelt og for at dette kan forblive tilfældet, påhviler der hver enkelt tilsluttet part et ansvar for ikke at være den ene part, der lukker uønsket trafik ind på sundhedsdatanettet.

5.2 Datasikkerhed på internettet

Der er flere måder at beskytte det lokale netværk på mod truslerne udefra. Først og fremmest via en router og en firewall

5.2.1 Router

Tilslutningen til Internet sker for alle lægepraksis vedkommende ved, at klinikken får opstillet mindst en router. Routeren har en forbindelse ud til Internet og en eller flere forbindelser ind til lokalnettet.

Konfigurationen af sikkerhedspolitikker sker ved, at leverandøren lægger aktuelle filtre ud i routeren. For at undgå at nogen forsøger at skaffe sig adgang til route-rens filtre, skal routeren altid være tændt og stå i et aflåst rum/skab.

5.2.2 Firewall

Lægepraksis har behov for en mere fleksibel sikkerhedsløsning end der kan opnås med en router, og der ønskes en større grad af sikkerhed. Firewall giver meget store muligheder for at kontrollere trafikken – både ud mod eksterne net og ind mod lokalnettet. De mere avancerede firewalls kan desuden undersøge dataindholdet i de enkelte TCP/IP-pakker og på den måde opdage, hvis nogen forsøger at kompromittere et netværk. Firewalls kan også sørge for at der bliver foretaget en logning af trafikken, således at man har materiale at gå ud fra i forbindelse med evt. efterforskning af sikkerhedsproblemer.

5.2.3 Personlige Firewalls

Med den stigende udbredelse af hjemme-pc-opkoblinger bør dette udstyr beskyttes af en sikkerhedspakke der indeholder en personlig firewall. Dels fordi hjemme-pc'en kan bruges som "springbræt" til at komme ind på klinikens netværk og dels fordi mange opbevarer fortrolige oplysninger på den lokale harddisk. Dette er i stigende grad en standardkomponent i de gængse operativsystemer (Windows etc.), men det er vigtigt ikke at slå denne funktion fra.

5.3 Trusler fra internettet

Datasikkerheden på det lokale net kan kompromitteres på flere måder udefra. I dette afsnit vil vi kigge på 5 forskellige trusselstyper og på, hvordan klinikkerne kan beskytte sig mod dem. I parentes er anført, hvilke sikkerhedsmæssige problemer de enkelte typer kan forårsage.

- usikre websider (indtastede oplysninger registreres, virus)
- e-mail (uretmæssig brug af mail-server, virus)
- portscanning (hel eller delvis kontrol med en server placeret inden for Firewall, fx adgang til andre servere eller afsendelse af spam-mail med klinikken som afsender)
- sniffing (aflytning af passwords, e-mail og trafik, mulighed for ulovlig adgang til informationer)
- malware (sletning af filer, misbrug af kapacitet, spredning af ondsindet kode, overvågning, indhentning og distribuering af kritiske informationer)

5.3.1 Malware

Malware er sammentrækningen af ordene ”Malicious Software” og er i dag en fællesbetegnelse for alt ondsindet programkode. Det skyldes, at hackeren i dag er så dygtige til at udvikle disse angrebsprogrammer, at de gamle definitioner (virus, trojanere etc.) ikke længere rækker. Med den stigende brug af internettet som informationskilde, både privat og erhvervsmæssigt, så har hackerne også udvidet deres jagtmarker. Skadelig kode kan dermed introduceres direkte som filer på kendt vis – men også gennem specielt udformet programkode placeret på Websider. Disse web-sider kan både være sociale netværk som Facebook – eller dedikerede angrebssites.

5.3.2 Port-scanning

5.3.2.1 Starten på et hackerangreb?

Angreb udefra mod ens lokalnet starter oftest med, at hackeren har foretaget en portscanning af nettet. Først checker portscanneren (fra et vilkårligt sted på internet), om der er nogen IP-adresser, der svarer. Et positivt svar betyder, at der er liv i maskinen med den pågældende IP-adresse, og at den er på nettet. Med svaret følger også informationer om styresystemet. Herefter checker portscanneren, hvilke porte, der lyttes på. En web-server vil lytte på TCP port 80, en mailserver på port 25/110 osv.

Portscannere er ofte kombineret med audit software, der efterfølgende går ind og analyserer det fundne – fx. holder dem op mod kendte svagheder på det relevante styresystem. Har hackeren først en oversigt over de aktive porte, er der et godt grundlag for at sætte angrebet ind, hvor det pågældende styresystem har kendte svagheder (exploits). Derved kan hackeren få hel eller delvis kontrol med maskinen og dermed stort set frit slag, både på lokalnettet og på internettet.

5.3.2.2 Sikring mod portscanning

Det er muligt vha. ens firewall at skjule alle åbne porte på lokalnettet for omverdenen på nær de åbninger, der er konfigureret i filteret i routeren/firewallen.

5.3.2.3 Sårbarhed og opdatering

For at undgå angreb er det vigtigt at vedligeholde serveren ved at opdatere systemerne med patches – dvs. små delprogrammer, der udfylder svaghederne. Her kan CERT (se ordliste) hjælpe til både med oplysninger om sårbarheder og med hjælp i konkrete tilfælde.

5.3.3 Sniffing

Med sniffing kan man aflytte trafikken på netværket og opsnappe passwords, e-mail, www og trafik til og fra netværksdrev.

Opsnapper man passwords, kan man misbruge disse til at få ulovlig adgang til andre systemer. Kigger man efter e-mail eller Instant Messenger (MSN Messenger), vil man både kunne se, hvad andre skriver, og hvem de skriver til. Hvis man aflytter web-trafik, vil man kunne se de sider, som andre går ind på – også selvom de er beskyttet med password. Holder man øje med netværksdrev, kan man se indholdet af filer, der bliver hentet eller gemt via netværket.

Man kan sniffe al trafik, som kommer forbi den netværksledning man sidder på. I praksis vil det sige al trafik på det pågældende lokalnet, med mindre der aktivt er gjort noget for at sikre sig.

5.3.3.1 Hvordan sniffer man?

Selve sniffingen foregår ved, at man installerer et program – en sniffer – der lytter til trafikken på ens netkort. Programmet opsamler så al den information, der suser forbi på nettet. De lidt mere avancerede programmer kan sættes op til at sortere i informationen, og man kan fx bede den om kun at kigge efter passwords eller breve, der indeholder lægens navn.

Man skal have adgang til en maskine eller netværksudstyr på nettet for at kunne sniffe. Fjendtlig sniffing kan ske enten fra en bærbar pc eller fra en hacket maskine. Den bærbare pc kan være indsmuglet af en person, der har adgang til lægepraksis. Han skal blot bruge et uopmærksomt øjeblik for at kunne sætte den bærbare et sted, hvor der er adgang til netværket. En mere skjult måde er at sniffe på trådløse opkoblinger.

Den hakede maskine kan være en arbejdsstation, hvor en medarbejder har hentet et (sjovt) program, der uheldigvis indeholder en trojansk hest (se ordliste). Når medarbejderen kører programmet, installerer det automatisk en sniffer, som medarbejderen ikke kommer til at mærke mere til. Når programmet har sniffet nok, kan det fx sende de opsamlede oplysninger via internettet til hackerens anonyme mailboks. En maskine kan også hackes uden downloading – se afsnit 5.3.2 i dette kapitel om portscanning.

Det er svært at sikre sig 100% mod sniffing. Heldigvis kan man begrænse snifferens kraft på to måder:

- ved at kryptere data
- ved at alle data ikke kommer forbi alle maskiner.

5.3.4 Kryptering

Hvis man krypterer data, er det lige meget, om trafikken kan aflyttes, idet data er forvanskede til ukendelighed. Kryptering kan laves på flere måder. Man kan

bruge de færdige programmets indbyggede kryptering, eller man kan få al sin netværkskommunikation krypteret. Hvis man krypterer netværkstrafikken, skal modtageren være i stand til at dekryptere trafikken igen. Dette kan fx gøres med VPN (Virtual Private Network), der er en standardfunktion i mange firewalls idag.

6 Driftssikkerhed

6.1 Beskrivelse af ansvar og opgaver

Som udgangspunkt skal klinikkens it-udstyr være i drift altid, og derfor er det vigtigt, det på forhånd er aftalt, hvem der har ansvar for forskellige funktioner som fx:

- Brugeroprettelse og brugerrettigheder
- Opdateringer af software
- Sikkerhedskopieringer
- Virusbeskyttelse
- Licensstyring

6.2 Malware beredskab

Da malwareangreb kan have meget store konsekvenser for en stabil driftssituation, bør klinikken abonnere på et sikkerhedsprogram, som dagligt får opdateret signaturfiler og regler.

6.3 Dokumentation

Enhver it-installation bør være veldokumenteret, således at en reetablering af systemet ikke er afhængig af en eller flere personers hukommelse.

En sådan dokumentation bør som minimum indeholde følgende:

- Topologitegning over netværket eller netværkene
- Adresseplan (IP-adresser)
- Konfiguration af servere og arbejdsstationer
- Revisionsændringer med dato og beskrivelse af ændringen
- Definerings af ansvarsområder

7 Ordliste

anti IP-spoofing filter

Forhindrer forfalskning af en arbejdsstations IP-adresse. Router kan udstyres med anti IP-spoofing filter.

arbejdsstation

Den computer, brugeren arbejder ved. Begreberne arbejdsstation, pc og computer dækker samme enhed i vejledningen.

audit software

Software, der analyserer trafikken på et netværk og giver alarmer, hvis der observeres "mistænkelig" trafik.

BIOS

Står for Basic Input Output System. BIOS'en er et lille stykke program, der ved opstart af maskinen fortæller softwaren (typisk Windows), at der er tilsluttet skærm, tastatur, mus osv.

boote

Udtrykket betyder egentlig "at tage støvlerne på". I overført betydning: at starte computeren – enten fra harddisk eller et løst medium, som f.eks. diskette, CD eller USB-nøgle.

brugerkonto

På en netværksserver bliver alle brugere oprettet med en brugerkonto, der definerer, hvilke rettigheder den enkelte bruger har.

CERT

Står for Computer Emergency Response Team, et verdensomspændende netværk, der har som opgave at hjælpe imod angreb på computere. Se yderligere på www.cert.dk

firewall

Server med særlig software, som kan begrænse, hvilke brugere der skal have adgang til hvilke programmer/tjenester på et givent tidspunkt. De mere avancerede firewalls kan kontrollere de enkelte IP-pakker for at se, om de indeholder virus. De fleste firewall kan etablere VPN forbindelser.

hacking

Forsøg på uautoriseret adgang til netværk.

hardware-baseret

Når vi skriver at en firewall, VPN-koncentrator og lignende i en række tilfælde bør være hardware-baseret, menes at disse funktioner varetages af små stykker udstyr, der er separate fra pc'er og servere. Dette er i modsætning til software-baserede firewalls etc., der er programmer, installeret på de pc'er og servere, der også anvendes til andre formål. Når vi i en række tilfælde anbefaler hardware-baserede sikkerhedskomponenter, er det fordi chancen for kompromittering af disse enheder alt andet lige er mindre end for tilsvarende software-baserede komponenter.

hub

For at undgå mange lange netværkskabler etableres en netværkstopologi, hvor der trækkes et kabel fra serveren til et eller flere centrale fordelingssteder. Her placeres enten en hub eller en switch, der er en boks med flere udtag.

IP-nummer

Internet Protocol number. IP-nummeret angiver en unik adresse på internet. Nummeret består af fire talgrupper, hver i intervallet 0 til 255, adskilt af punktummer.

Fx 130.228.8.233

krydsfelter

Fysisk samlings- og delingspunkt for kabler for arbejdsstationer, server, printere osv. i et netværk.

LAN

Står for Local Area Network, klinikkens lokale netværk.

logfil

Datafil, hvor der gemmes oplysninger om, hvilken aktivitet der er foregået fra en given arbejdsstation

malware

Sammentrækningen af ordene ”Malicious Software”, ondsindet programkode, og bruges i dag til at beskrive alt programkode der kan bruges ved hackerangreb.

netværkstopologi

Betegnelse for et netværks opbygning: Hvilke elementer det består af (servere, hubs, routere osv.), og hvordan de er forbundet.

orme

Orme er en virustype, som spredes uden at en bruger er involveret.

ping

Oprindelig det lydsignal en ubåd sendte ud for at måle afstanden til et mål ved at måle tiden fra afsendelsen af signalet, til det kom retur. Bruges på nettet til at måle svartiden fra en given vært.

router

Enhed, der (oftest) kan etablere VPN forbindelser og sørger for at sende trafikken i den rigtige retning.

spam-mail

Kan sammenlignes med uopfordrede reklamer. Spam-mail foregår ved at afsenderen sender enslydende, meningsløse, breve til mange modtagere.

server

Maskine, der deler nogle af sine ressourcer med andre maskiner på netværket.

smileys

Når man skriver sammen på nettet, er det ikke muligt at bruge ansigtsudtryk og tonefald til at understrege, hvad man mener. Man bruger derfor i stedet smileys til at understrege en stemning, når man chatter på nettet og sender e-mail.

Smileys kan fx se sådan ud :-)

switch

Fordelingsenhed til netværk. Indeholder ofte mere ”intelligens” end en hub.

trojanske heste

En ”trojansk hest” er et program, der ser uskyldigt ud, men som samtidig udfører ubehagelige handlinger, eksempelvis medbringer en virus eller installerer et bagdørsprogram.

VPN

Står for Virtual Private Network, et privat netværk, der ligger oven på det offentlige internet. Servere inden for det private netværk kommunikerer indbyrdes i krypterede tunneller, der forhindrer servere uden for VPN'et i at aflytte trafikken.